IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

DENIS ZHIROVETSKIY, individually and on behalf of similarly situated individuals, *Plaintiff,* v. ZAYO GROUP, LLC, a Delaware limited liability company, *Defendant.*	)	No. 17-cv-05876 Hon. Sharon Johnson Coleman

FIRST AMENDED CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff Denis Zhirovetskiy ("Plaintiff"), individually and on behalf of other similarly situated individuals, brings this First Amended Class Action Complaint against Defendant, Zayo Group, LLC ("Zayo" or "Defendant"), to stop Defendant's collection, use, and storage of his and other consumers' sensitive biometric information in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. ("BIPA"), and to obtain redress for all persons aggrieved by its conduct. Plaintiff alleges as follows based on personal knowledge as to his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

INTRODUCTION

1. This case concerns Zayo's regular practice of capturing, collecting storing and using Plaintiff's and other consumers' biometric identifiers and biometric information without regard to the regulations imposed by BIPA and the concrete privacy rights and pecuniary interests that BIPA protects.

2. Recognizing the serious harm that can come from unregulated collection and use of biometrics, in 2008 Illinois passed BIPA, a statute of reasonable regulations addressing the collection, use and retention of biometric identifiers and biometric information by private entities, like Zayo.

3. A factor that influenced the Illinois Legislature in passing BIPA was the 2007 bankruptcy of a company that specialized in the collection and use of biometric information and the subsequent fear of the risk of millions of digital fingerprint records being disseminated or sold to unknown parties. Legislators feared this would happen without knowledge or consent of the individuals whose biometrics were obtained and would result in such persons having no knowledge of where their biometrics were or how they were being used. The Illinois Legislature passed BIPA to provide consumers with statutory protection of their privacy rights; to ensure that they would receive certain disclosures before a private entity could collect, obtain and/or use their biometrics; to decrease the risk of a misappropriation of one's identity or a similar compromise of one's privacy; and to ensure that individuals whose biometrics were being collected, obtained and/or used could provide informed consent and be fully aware of how their biometrics were being handled and disposed of.

4. Indeed, the Illinois Legislature passed BIPA in part because "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information". 740 ILCS 14/5. For example, even sensitive information like Social Security numbers, when compromised, can be changed. "Biometrics, however, are biologically unique to each individual and therefore, once compromised, such individual has no recourse, is at a heightened risk for identity theft, and is likely to withdraw from biometric facilitated transactions." *Id.*

5. BIPA defines a "biometric identifier" as any personal feature that is unique to an individual and includes fingerprints, iris scans, palm scans, and DNA, among others. Under BIPA "biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier which is used to identify an individual. 740 ILCS § 14/10.

6. As technology has continued to develop over the past decade, biometrics are becoming more mainstream and are no longer relegated to esoteric corners of commerce. Many businesses and financial institutions have incorporated biometric applications into their consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

7. BIPA provides, *inter alia*, that a private entity such as Defendant may not obtain and/or possess an individual's biometrics unless it first:

(1) informs that person in writing that biometric identifiers or biometric information will be collected or stored;

(2) informs that person in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being collected, stored and used; and

(3) receives a written release from the person for the collection of their biometric identifiers or biometric information.

8. A private entity in possession of biometric identifiers or biometric information is also required to publish a publicly available written retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. 740 ILCS 14/15.

9. For companies wishing to comply with BIPA, such compliance is straightforward and the necessary disclosures and written release can be easily achieved through a single signed sheet of paper.

10. Defendant is a telecommunications service provider and operator of data storage facilities throughout the nation. Choosing to shun more traditional security measures like checking ID's, Defendant maintains a mandatory and invasive security protocol that relies on the collection, storage, and use of consumers' biometric identifiers and biometric information, while failing to follow the reasonable regulations set by the BIPA and disregarding and the serious privacy interests they protect.

11. The threat of a security breach resulting in the loss of data is significant and Defendant acknowledges as much in its 2017 annual 10k report to the Securities and Exchange Commission. In the report, under the section titled "Risks Related to Our Business," Defendant lists "physical or electronic security breaches" as well as "sabotage and vandalism." These risks are more than mere hypotheticals and include digitized biometric information. For example, in 2015, Zayo was the target of repeated attacks against its underground data infrastructure. According to a *Fortune* story detailing the attacks against Zayo's internet capabilities, the "concerted strike" was "particularly alarming" and severed consumer access to the internet.[1]

12. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting, storing, and using Plaintiff's and other similarly situated consumers' biometric identifiers and/or biometric information in direct violation of the BIPA. 740 ILCS § 14/10.

13. On behalf of himself and the proposed Class defined below, Plaintiff seeks an injunction requiring Defendant to cease all unlawful activity related to its collection, storage, use and possession of biometric identifiers and/or biometric information and an award of statutory damages to the Class members, together with costs and reasonable attorneys' fees.

[1] http://fortune.com/2015/07/01/cutting-internet-cables/.

PARTIES

14. Defendant, an operator of data storage facilities in Illinois and elsewhere throughout the nation, is a Delaware corporation that conducts business in Illinois.

15. Plaintiff is a resident and citizen of the state of Illinois.

JURISDICTION AND VENUE

16. This Court has diversity jurisdiction under 28 U.S.C. § 1332(d), because (i) at least one member of the putative class is a citizen of a state different from any Defendant, (ii) the amount in controversy exceeds $5,000,000 exclusive of interests and costs, and (iii) none of the exceptions under that subsection apply to the instant action.

17. This Court has personal jurisdiction over Defendant because Defendant transacts business in Illinois and because a substantial part of the events giving rise to Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Defendant captured Plaintiff's biometric identifiers and/or biometric information in this State.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred in this District, as the Defendant captured Plaintiff's biometric identifiers and/or biometric information at one of its data storage centers located in this District.

BACKGROUND

19. Illinois enacted BIPA to regulate entities such as Defendant that collect, store and use biometric identifiers and biometric information, including fingerprints, iris scans, and handprints.

20. Under BIPA, a private entity may not collect, capture, purchase, receive through trade, or otherwise obtain a person's biometric identifier or biometric information unless it first:

(1) Informs the person in writing that a biometric identifier or biometric information is being collected;

(2) Informs the person in writing of the specific purpose and length of time for which a person's biometric identifier or biometric information is being collected, stored and used; and

(3) Receives a written release executed by the subject of the biometric identifier or biometric information.

740 ILCS 14/15(b).

21. Section 15(a) of the BIPA also requires that a private entity in possession of biometric identifiers or biometric information develop:

a. A written policy;

b. Available to the public;

c. Which establishes a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information;

d. Within three years of the individual's last interaction with the private entity, or when the initial purpose of for collecting or obtaining biometric identifiers and biometric information has been satisfied.

740 ILCS 14/15(a).

22. Defendant is a "private entity" as that term is defined under the BIPA. *See* 740 ILCS 14/10.

23. Defendant is constructively, if not actually, in possession of Plaintiff's and other consumers' biometric identifiers and/or biometric information. Defendant not only possesses such

biometrics but also advertises – and profits from – the fact that its data centers utilize biometrics for security purposes.

24. While most businesses secure their facilities through traditional methods, such as ID cards and key codes, Defendant uses consumers' handprints and other biometric identifiers and biometric information to identify and approve them for entry into its data centers. Defendant accomplishes this through the use of biometric scanning devices, which capture, store and use consumers' biometrics in the form of handprints. These handprints and the data gleaned from them constitute biometric identifiers and/or biometric information as defined by BIPA. Every time a consumer accesses one of Defendant's biometrically-secured facilities, Defendant captures, collects or otherwise obtains and/or uses his/her biometric identifiers and/or biometric information in violation of BIPA.

25. Unlike ID cards or key codes—which can be changed or replaced if stolen or compromised—handprints are unique, permanent biometric identifiers associated with the individual. The capture, storage, use and potential dissemination of these permanent biometric identifiers in violation of BIPA exposes Plaintiff and consumers to serious and irreversible privacy risks and deprived them of the ability to make an informed decision with respect to providing their biometric identifiers and/or biometric information.

26. As the recent Equifax Data Breach has made clear, digitally stored information is notoriously difficult to protect and its dissemination can have disastrous consequences. This is particularly true with biometrics, as the privacy risks associated with biometrics are unparalleled; such information is more sensitive than even a person's social security number because it cannot be changed.

27. BIPA regulates the possession of biometrics by, among other things, requiring companies to develop retention policies related to the storage of biometrics and mandating that such information be destroyed within three years of an individual's last interaction with the company.

28. BIPA also regulates *how* entities obtain individuals' biometrics. BIPA requires companies to not only provide certain disclosures to individuals, but also requires that they obtain a written release from individuals prior to collecting their biometric identifiers and/or biometric information.

29. Specifically, BIPA requires entities to inform individuals not only that their biometrics will be collected or stored, but also of the purpose and length of term such information will be collected, stored, and used. The statute also requires that entities receive a written release from individuals and that they make a schedule for retaining and destroying such biometric identifiers and biometric information available to the public. In this way, BIPA is specifically designed to decrease the risk of privacy violations to individuals whose biometrics are being captured, stored, and/or used. It also designed to protect those individuals' right to be informed with respect to the collection and use of their biometric identifiers and biometric information, and allows them to make better informed decisions as to the circumstances under which they agree to provide their biometric identifiers and/or biometric information.

30. BIPA is not a particularly prohibitive statute, and its narrowly tailored provisions do not place an absolute bar on the collection, capture or transmission of biometric data. However, BIPA does provide individuals with a private right of action so that they have a vehicle for protecting their right to privacy in their biometric identifiers and biometric information and for protecting their right to know the precise ways their biometric identifiers and biometric

information will be used and disposed of. To effectuate this purpose BIPA simply mandates that entities which *elect* to engage in the use of biometric systems do so with reasonable, disclosed safeguards and only *after* receiving informed consent from the individual to take such biometric identifiers and/or biometric information.

31. Defendant's practices of collecting, obtaining, capturing, storing and using Illinois residents' biometric identifiers and/or biometric information are unlawful under the BIPA because such practices fail to obtain a written release from individuals prior to collecting their biometric identifiers and/or biometric information and fail to provide the disclosures required by BIPA. Defendant's practices therefore violate the specific statutory requirements of BIPA and severely infringe on consumers' right to privacy with regard to their biometric identifiers and biometric information.

FACTS SPECIFIC TO PLAINTIFF

32. During the relevant period, Plaintiff was sent by his employer to one of Defendant's many data centers located in Illinois so that he could perform maintenance on his employer's data servers which were located inside Defendant's facility. As a condition of entry into Defendant's facility and for purported security purposes, Plaintiff was required to submit to a mandatory and invasive biometric hand-scan before he was permitted access to the part of the facility where his employer's servers were stored.

33. Plaintiff was hesitant to provide his biometric identifiers and/or biometric information to Defendant and was concerned about what would become of his extremely personal information. Nevertheless, because Plaintiff was required to access Defendant's facility so that he could perform work on behalf of his employer, he did not feel as though he had an option as to providing his biometrics to Defendant.

34. Defendant then captured Plaintiff's biometric identifier and/or biometric information by scanning Plaintiff's handprint into its biometric security system without receiving informed written consent from Plaintiff as required by BIPA. Plaintiff's handprint and the biometric information Defendant obtained from it was then stored, associated with his identity and used by Defendant to identify Plaintiff and to provide access to its data center.

35. After Plaintiff's handprint was initially captured, stored, used, and associated with his identity, Defendant required Plaintiff to scan his handprint into one of its biometric security devices as a condition of Plaintiff's access to its data center. Plaintiff subsequently visited Defendant's data center on several occasions, and on each occasion Plaintiff's biometrics were captured, stored and/or used by Defendant.

36. Defendant failed to inform Plaintiff in writing that they were collecting or storing his biometric identifiers and/or biometric information.

37. Defendant also failed to inform the Plaintiff in writing of the specific purpose and length of time for which his biometric identifier and/or biometric information was being stored and used prior to capturing or collecting such information.

38. Plaintiff was never provided with, nor did he ever sign, a written release allowing Defendant to collect, store or use his handprint and related biometric information.

39. Prior to taking Plaintiff's biometric data and/or information Defendant also failed to make a written policy available to Plaintiff or any other members of the public that established a retention schedule and guidelines for permanently destroying the biometric identifiers and biometric information that it collects, as required by the BIPA. 740 ILCS 14/15(a).

40. Defendant further failed to obtain written consent from Plaintiff for Defendant's transmission of Plaintiff's biometrics to any third parties, including outside vendors. Defendant

has also violated BIPA on each occasion it transmits such information to third parties without consumers' consent.

41. To this day, Plaintiff is unaware of the status of his biometric identifiers and biometric information that were obtained by Defendant. Defendant has not informed Plaintiff whether it still retains his biometric identifiers and/or biometric information, and if so, for how long it intends to retain such information without Plaintiff's consent, or how such information is to be treated in the event Defendant is acquired, sold or declared bankrupt.

42. By knowingly and willfully failing to comply with BIPA, Defendant has violated consumers', including Plaintiff's, substantive privacy rights, and as a result, Plaintiff and the other members of the Class have continuously been exposed to ongoing privacy invasion, with such constant risk of exposure constituting a severe harm and violation of their rights.

43. A flurry of recent activity at Zayo, including insider stock sales in which the CEO sold $10 million worth of Zayo stock, high-level executive departures, and weak corporate earnings have alerted investors to possible trouble. These factors, combined with Zayo's history of "net losses since our inception" and the fact that they "may not be able to generate enough cash flow to meet [their] debt obligations," all increase the likelihood of future bankruptcy or the need to sell assets which might include Plaintiff's biometrics.

44. As a result of Defendant's conduct, Plaintiff has also experienced bodily injury in the form of mental anguish and anxiety. For example, Plaintiff has experienced mental anguish and injury when he thinks about what would happen to his biometric information if Defendant went bankrupt or otherwise sold its assets; when he wonders whether Defendant will ever delete his biometric information; and when he wonders what would happen to his information and identity if Defendant were to experience a data breach, such as the one recently experienced by

Equifax. This harm is even more acute because an individual with access to his biometrics could potentially access other accounts which may currently, or at some time in the future, be secured through his biometrics.

45. Defendant's failure to adhere to BIPA regulations addressing the collection, use, safeguarding, handling, storage, retention and destruction of biometric identifier and biometric information is not only harmful to Plaintiff, it has also created a public harm because it has and will continue to decrease the public's trust in the gathering and use of biometrics even when used for legitimate purposes and in accordance with all relevant laws, an outcome the Illinois Legislature sought to avoid. 740 ILCS 14/5 (g).

46. Plaintiff's concern for the whereabouts of his biometric identifiers and/or biometric information has also caused him to become leery of and less likely to participate in future biometric transactions involving a third party, a result that the legislature was specifically attempting to avoid by enacting BIPA. 740 ILCS 14/5 (c).

47. Because BIPA was specifically enacted to regulate an entity's capture, collection, storage and use of biometric identifiers and/or biometric information, and because Plaintiff and the other putative class members' biometric identifiers and/or biometric information were captured, collected or otherwise obtained, and possessed by Defendant, all such individuals have been aggrieved by Defendant's conduct in violation of the statute.

CLASS ALLEGATIONS

48. Plaintiff brings this action on behalf of himself and similarly situated individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure. Plaintiff seeks to represent a Class defined as follows:

> All individuals whose biometric identifiers and/or biometric information was captured, obtained, stored or used by Defendant within the state of Illinois during

the applicable limitations period.

49. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

50. Upon information and belief, there are hundreds, if not thousands, of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiff, the members can be readily identified through Defendant's records.

51. Plaintiff's claims are typical of the claims of the Class members he seeks to represent, because the factual and legal bases of Defendant's liability to Plaintiff and the other Class members are the same, and because Defendant's conduct has resulted in similar injuries to Plaintiff and to all of the other members of the Class. As alleged herein, Plaintiff and the other putative Class members have all been subjected to the same conduct by Defendant and have all suffered damages as a result of Defendant's BIPA violations.

52. There are many questions of law and fact common to the claims of Plaintiff and the other Class members, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant informed Class members in writing that it was collecting and storing their biometric identifiers and/or biometric information;

b. Whether Defendant obtained a written release from Class members before capturing, collecting, or otherwise obtaining their biometric identifiers or biometric information;

c. Whether Defendant developed and made available to the public a written policy which establishes a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information;

d. Whether Defendant provided a written disclosure to consumers that explains the specific purpose and the length of term, for which their biometric identifiers and biometric information are being collected, stored and used;

e. Whether Defendant's conduct violates the BIPA;

f. Whether Defendant's violations of the BIPA are willful and reckless; and

g. Whether Plaintiff and the Class members are entitled to damages and injunctive relief.

53. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive, and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

54. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class.

55. Defendant has acted and failed to act on grounds generally applicable to the Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to

ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNTS I - VI

Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*., (on behalf of Plaintiff and the Class)

56. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

57. Illinois' BIPA requires companies to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

58. BIPA also requires that companies in possession of biometric data establish and maintain a publicly available retention policy. Entities such as Defendant that possess biometric data must (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (companies may not retain data longer than three years after the companies' last interaction with the customer); and (ii) must adhere to the publicly posted retention and deletion schedule.

59. Defendant is a private entity under the BIPA.

60. Plaintiff and the other Class members had their "biometric identifiers," including handprints, collected, captured, received or otherwise obtained by Defendant. Plaintiff and the other Class members' biometric identifiers were also used to identify them, and therefore constitute "biometric information" as defined by the BIPA. 740 ILCS 14/10.

61. Each instance when Plaintiff and the other Class members scanned their handprints into Defendant's biometric security devices, Defendant captured, collected, stored, and used Plaintiff's and the Class members' biometric identifiers or biometric information without lawful consent as required by BIPA.

62. Defendant's practices with respect to capturing, collecting, storing and using biometric identifiers and information fail to comply with applicable BIPA requirements. Specifically, Defendant failed to adhere to the following BIPA requirements, with each such failure constituting a separate and distinct violation of BIPA and a separate and distinct cause of action:

I. Defendant failed to inform Plaintiff and the members of the Class in writing that their biometric identifiers or biometric information were being collected and stored, as required by 740 ILCS 14/15(b)(1);

II. Defendant failed to inform Plaintiff and the members of the Class in writing of the specific purpose for which their biometric identifier or biometric information was collected, stored and used, as required by 740 ILCS 14/15(b)(2);

III. Defendant failed to inform Plaintiff and the members of the Class in writing of the specific length of term their biometric identifier or biometric identifiers were collected, stored and used, as required by 740 ILCS 14/15(b)(2);

IV. Defendant failed to obtain the written release required by 740 ILCS 14/15(b)(3);

V. Defendant failed to provide a publicly available retention schedule detailing the length of time biometric identifiers and biometric information is stored or guidelines for permanently destroying the biometric identifiers and biometric information it stores, as required by 740 ILCS 14/15(a); and

VI. Defendant failed to obtain consent to disclose or disseminate the Class members' biometric identifiers or biometric information as required by 740 ILCS 14/15(d)(1).

63. By designing and operating a security system based on biometrics that was devoid of the consumer protections required by BIPA and by advertising such security systems to attract customers, Defendant profited from Plaintiff's and the Class members' biometric identifiers and biometric information in violation of 740 ILCS 14/15(c).

64. By collecting, storing, and using Plaintiff's and the other Class members' biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the other Class members' respective rights to privacy in their biometric identifiers or biometric information as set forth in BIPA, 740 ILCS 14/15(a), and caused mental anguish and other damages to Plaintiff and the other Class members.

65. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of the BIPA and, alternatively, damages of $1,000 for each negligent violation of the BIPA. 740 ILCS 14/20(1).

66. Defendant's violations of the BIPA, as set forth herein, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with the BIPA disclosure, consent, dissemination, and policy posting requirements.

COUNT VII
Negligence
(On behalf of Plaintiff and the Class)

67. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

68. Defendant owed Plaintiff and the putative Class a reasonable duty of care in its capture, collection, storage, use and possession of Plaintiff's biometric identifiers and/or biometric information. Under this duty Defendant was required to collect, capture, use and store Plaintiff and the Class's biometric identifier and/or biometric information in compliance with the regulations set forth in BIPA.

69. Defendant breached it duty, which was informed by the BIPA requirements promulgated by the Illinois Legislature, by failing to implement reasonable procedural safeguards surrounding the collection and use of Plaintiff's and the Class members' biometric identifiers and/or biometric information.

70. Specifically, Defendant breached its duty by failing to provide Plaintiff and the Class members in writing of the specific purpose and length of time for which their respective handprints were being collected, stored and used, as well as by failing to obtain Plaintiff's and the Class members' prior written consent before collecting their biometric identifiers and/or biometric information.

71. Defendant also breached its duty by failing to provide a retention schedule and guidelines for permanently destroying Plaintiff's and the Class members' biometric identifiers and biometric information.

72. Defendant's breach of its duty of care proximately caused the ongoing violation of Plaintiff's and the Class members' right to privacy.

73. Defendant's breach of its duty proximately also caused and continues to cause Plaintiff and the other Class members mental anguish and mental injury. For example, Plaintiff experiences mental anguish and injury when thinking about what would happen to his biometric identifiers and biometric information if Defendant went bankrupt or otherwise sold its assets; when he wonders whether Defendant will ever delete his biometric information; and when he wonders what would happen to his information and identity if Defendant were to experience a data breach, such as the one recently experienced by Equifax.

74. Accordingly, Plaintiff seeks damages in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, respectfully requests that this Court enter an Order:

a. Certifying the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;

b. Declaring that Defendant's actions, as set forth herein, violate BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with the BIPA requirements for the collection, storage, use and possession of biometric identifiers and biometric information;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(1);

e. Awarding statutory damages of $1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(3);

f. Awarding reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);

g. Awarding pre- and post-judgment interest, as allowable by law; and

h. Awarding such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Dated: October 10, 2017

Respectfully Submitted,

DENIS ZHIROVETSKIY, individually and on behalf of a class of similarly situated individuals

By: /s/ David L. Gerbie
One of His Attorneys

Myles McGuire
Evan M. Meyers
David L. Gerbie
MCGUIRE LAW, P.C.
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
mmcguire@mcgpc.com
emeyers@mcgpc.com
dgerbie@mcgpc.com

Attorneys for Plaintiff and the Putative Class